REMARKS

REQUEST TO *WITHDRAW THE FINALITY* OF THE 7/16/07 OFFICE ACTION

The Applicant respectfully requests the withdrawal of the finality of the current Final Office Action mailed on July 16, 2007, on the basis that the Final Office Action was premature, for at least the following reasons.

In the rejection of Claim 1 based on *Phan*, *Walsh*, and *Boldon*, the Final Office Action correctly notes that the combination of *Phan* and *Walsh* does not disclose "the virus scanning being taking place on the MFP," but then the Final Office Action thereafter fails to address the "virus protection process executing in the memory and being configured to…detect…and in response to detecting…, perform one or more actions…," although the Applicant notes that in an earlier portion of the Final Office Action, these features are addressed and alleged to be disclosed by *Walsh*, not *Boldon*.

Instead of addressing these features of Claim 1 and providing a basis for rejecting these features based on *Boldon* or addressing how Boldon discloses "virus scanning…on the MFP," the Final Office Action states that *Boldon* discloses "a memory storing device instructions which, when processed by one [or] more processors, causes the multi-function peripheral to perform the steps of (paragraph 0016, lines 8-12) detect that a request for data to be analyzed for viral infection has been received over a network from a network device (paragraph 0019, lines 3-7; paragraph 0016, lines 5-8); and in response to detecting receipt of the request, providing data from the multi-function peripheral device to the network device over the network (paragraph 0016, lines 12-14)." These cited features, although appearing to come from a claim, do ***NOT*** come from any claims of the present Application, nor do these features come from *Boldon* itself.

Also, these features cited in the Final Office Action are very different than those of pending Claim 1 in the present Application. Specifically, in Claim 1, the features omitted from the rejection concern a virus protection process, which is comprised within the multi-function peripheral, is configured to "detect that one or more unauthorized instructions have been stored on the multi-function peripheral device" and "in response to detecting that the one or more unauthorized instructions have been stored on the multi-function peripheral device, perform one or more actions to address the one or more unauthorized instructions that have been stored on the multi-function peripheral device."

In contrast, the features being referred to in the Final Office Action's rejection of Claim 1 concern detecting that a request for data has been received, in which the requested data is to be analyzed for viral infection, and in response to detecting the request, providing the data to a network device. Note that these features do not include a step of detecting whether unauthorized instructions are present in the data, nor do these features include performance of any actions to address a viral infection that might be detected. However, in the approach of Claim 1 of the present application, the multi-function peripheral comprises the virus detecting process that detects whether unauthorized instructions are stored on the MFP and then taking one or more actions to address the unauthorized instructions.

After some investigation, the Applicant has determined that these features being cited in this portion of the rejection of the Final Office Action and alleged to be disclosed in *Boldon* but that are not actually included in Claim 1 of the present Application, have instead been taken from an Office Action in another pending application being examined by another Examiner within Art Unit 2109. Specifically, the Applicant has determined that this portion of the Final Office Action mailed July 16, 2007 for the present Application was apparently copied from the first non-final Office Action mailed February 22, 2007 in the related Application, S/N 10/776,486. In particular, the copied portion is from page 6, item 8, which is the 102(b) based rejection using *Boldon* for Claim 1 of that related Application. (The Applicant notes that this related Application has subsequently received a Final Office Action mailed on July 6, 2007.)

Thus, as the Final Office Action currently stands, the basis of the rejection of Claim 1 is based on reading into a prior art reference, namely *Boldon*, the features of a claim, namely the "multi-function peripheral device… and so on," that is taken from another application, namely the related Application, S/N 10/776,486, and how those features of that other claim in the related Application were alleged to be disclosed by *Boldon*. Since the statement before this quotation from the first non-final Office Action of the related Application is that the combination of *Phan* and *Walsh* does not disclose "the virus scanning being taking place on the MFP," it appears to the Applicant that the Final Office Action is reading features of a claim from another application into the prior art reference of *Boldon*, and then based on that combination of the features of that claim with *Boldon*, rejecting Claim 1 of the current Application. The Applicant respectfully submits that there is no legal or administrative basis for reading claims of a different application into a prior art reference to reject the claims of the application undergoing examination.

While it appears to the Applicant that the Final Office Action intended to reject, based on *Boldon*, the features of Claim 1 that are not addressed in the rejection using *Phan* and *Walsh* in the earlier portion of the rejection, it is possible that the Final Office Action meant to use another reference entirely. Even if the Applicant were to proceed based on *Boldon* being the correct reference, the rejection of Claim 1 essentially becomes one of rejecting those features of Claim 1 on *Boldon* as a whole. However, in an Office Action "the particular part relied on must be designated as nearly as practicable ... The pertinence of each reference, if not apparent, must be clearly explained ..." (MPEP §707, citing 37 C.F.R. §1.104(c)(2)), and "the particular figure(s) of the drawings(s), and/or page(s) or paragraph(s) of the reference(s), and/or any relevant comments briefly stated should be included." (MPEP §707).

Thus, treating the rejection of the latter portion of Claim 1 as being based on *Boldon* as a whole, there is insufficient basis to provide the Applicant with adequate notice or reasonable particularity with respect to the basis of the rejections based on *Boldon*. Instead, the entirely of *Boldon* is essentially identified in a non-specific way. As a result, the Applicant has had to engage in guesswork to determine the basis of the rejection based on *Boldon*. And yet, the Applicant cannot see any structure or functions in the reference that correspond to the claims.

Furthermore, prior to the addressing *Boldon*, the Final Office Action correctly states that "Phan and Walsh et al. does not disclose the virus scanning being taking place on the MFP." Thus, it would appear that the Final Office Action is attempting to rely upon *Boldon* as disclosing virus scanning on an MFP. But the Applicant respectfully submits that this is not a correct interpretation of *Boldon* because *Boldon* only addresses virus filtering in a peripheral such as a printer, scanner, or facsimile machine (see Abstract), all of which are single function peripherals, not multi-function peripherals. Nowhere within *Boldon* has the Applicant been able to find a disclosure of an MFP. In contrast, *Phan* addresses the use of user interface addresses in an MFP, although as noted in the Final Office Action, *Phan* is silent as to the use of virus scanning on such MFP's. Thus, this disconnect between the apparent use of *Boldon* in an attempt to show virus scanning on an MFP when in fact *Boldon* says nothing about MFP's tends to lead the Applicant to believe that the reference to *Boldon* in the Final Office Action was meant to address some other prior art reference instead of *Boldon*.

As a result of the issues outlined above, the Applicant respectfully requests that the finality of the current Final Office Action be withdrawn because the final rejection is premature

(see MPEP §706.07(c) and (d)) because there is no prima facie basis for the Office's final rejection of Claim 1. In addition, the Applicant respectfully submits that the Final Office Action is premature due to the uncertaintly as to whether the Final Office Action in fact meant to rely upon *Boldon* and the apparent attempt, as the Final Office Action is written, to read into the prior art reference of *Boldon* unrelated features of a claim from another patent application. As the current Final Office Action stands, the basis for the rejection is unknown and would require guesswork on the part of the Applicant to determine whether or not the Office's position would warrant the Applicant pursuing an appeal, not to mention the problem of the apparent reading into *Boldon* of the claims from a different application.

In addition, the Applicant notes that the Pre-Appeal Brief Conference Program provides for "an opportunity to request a review of identified matters on appeal...The goals of the program are...(2) to identify the omission or presence of essential elements required to establish a prima facie rejection." Thus, as the Final Office Action currently stands, there is an omission of numerous features of Claim 1 that are required to establish the prima facie rejection because those features described above that are taken from the claims of another patent application are included in Claim 1 that is being rejected, and furthermore, that those features quoted from the claim of the other pending patent application are very different features from the claims of the present Application.

As a result, the Applicant respectfully submits that if the Applicant were to pursue an appeal, the appeal would be the type of case handled by the Pre-Appeal Brief Conference Program and would result in a reopening of prosecution to address the deficiencies and confusion in the rejection of Claim 1. However, to avoid the expense and delay involved in even pursuing a Pre-Appeal Brief Conference, the Applicant prefers to have the finality of the Final Office Action withdrawn and a new action on the merits issued that properly addresses all of the features of Claim 1 without relying on the features of a claim from a separate patent application and apparently reading those claim features of the other application into the content of the prior art reference being cited and relied upon by the rejection.

ENTRY OF THE AMENDMENTS

Assuming that the Applicant's request to withdraw the finality of the Final Office Action is granted, the Applicant respectfully requests the entry of the amendments included herein.

Regardless of whether or not the amendments herein are entered, the Applicant also respectfully requests that the next communication from the Office address the features of Claim 1 of the current Application, and not the features from a claim of a different application, if that next communication continues to rely upon *Boldon*.

SPECIFICATION

In the specification, paragraph [0020] has been amended to provide a typographical correction. Paragraph [0022] has been amended to include the descriptive label for element 112 from FIG. 1, namely "Application programs" 112. These amendments to the specification are fully supported by the application as filed, and no new matter is added.

STATUS OF CLAIMS

Claims 4-7, 10, and 12-14 have been cancelled.

Claims 1, 3, 9, and 11 have been amended.

Claims 16-28 have been added.

No claims have been withdrawn.

Claims 1-3, 8-9, 11, and 15-28 are currently pending in the application.

"TRANSFER" OF CLAIMS FROM RELATED APPLICATION

The Applicant notes that newly added Claims 17-28 are based upon claims previously pending in the related Application, S/N 10/776,486 and that those corresponding claims in the related Application have been cancelled. Thus, the Applicant has effectively transferred Claims 17-28 from Application S/N 10/776,486 into the present Application., and the Applicant respectfully suggests that further examination of the claims of the present Application take into account the previous examination of the additional claims from the related Application, S/N 10/776,486.

SUMMARY OF THE REJECTIONS

Based on the statements of the Final Office Action that (1) Claims 1-15 are rejected based on *Phan*, *Walsh*, and *Boldon*; (2) the previous non-final Office Action is to be used for the basis of the rejections of Claims 2-15; and (3) the details of the rejections of the previous non-final Office Action, the basis of the rejections of the Claims are understood by the Applicant to be as

given below. If the basis of the rejections differ from the following, the Applicant respectfully requests that the next communication from the Office state the basis for the rejections.

Claims 1-7 and 10-15 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Number 5,937,150 issued to Phan (" *Phan* ") in view of U.S. Patent Number 5,956,481 issued to Walsh et al. (" *Walsh* ") and in further view of U.S. Patent Application Publication Number 2003/0048468 A1 of Boldon et al. (" *Boldon* "). Based on the statement of the Final Office Action that references the previous Office Action for the basis of the rejections of Claims 2-15, Claims 8-9 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Boldon* in view of *Walsh* and in further view of *Phan* and still in further view of U.S. Patent Number 5,832,208 issued to Chen et al. (" *Chen* "). The rejections are respectfully traversed.

ARGUMENTS IN REPONSE TO THE REJECTIONS

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

As amended herein, Claim 1 features in relevant part:

"A multi-function peripheral device comprising:

.....[*features omitted for purposes of the following explanation only*]

a virus protection process executing in the memory and being configured to perform the steps of:

examine data stored on *non-volatile memory* of the multi-function peripheral device;

based on examining the data, detect that one or more **unauthorized instructions** are **stored on the non-volatile memory** of the multi-function peripheral device; and

in response to detecting that the one or more **unauthorized instructions** have been **stored** on the non-volatile memory of the multi-function peripheral device;

perform one or more actions to address the one or more unauthorized instructions that have been stored on the non-volatile memory of the multi-function peripheral device; and

wherein the one or more actions includes **rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device **by *moving* the one or more unauthorized instructions into a *protected area* of the *non-volatile memory***." (Emphasis added.)

Thus, Claim 1 features that the virus protection process is configured to "**examine data stored on *non-volatile memory***" and "**in response to detecting** that the one or more **unauthorized instructions** have been **stored**," **rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device **by *moving* the unauthorized instructions into a *protected area* of the *non-volatile memory***."

The amendments to Claim 1 are fully supported by the Application as filed, and no new matter is included. For example, Claim 1 has the features of previously pending, but now cancelled, Claims 6 and 10 incorporated, along with the additional feature of moving the one or more unauthorized instructions into a protected area of non-volatile memory, which is supported by Paragraph [0030].

(2) INTRODUCTORY DISCUSSION OF *WALSH*

In contrast to the approach of Claim 1, *Walsh* discloses a technique for protecting data files on a computer system from being infected by a virus by interrupting an "open file event" to determine "whether the file is ***likely*** to contain a virus," and if the file is determined to ***likely*** contain a virus, generate a notice to the user of that likelihood or risk, and if the file is not ***likely*** to contain a virus, completing the opening of the file. (Abstract; emphasis added.) Importantly, ***Walsh* is *not* directed to the detecting of viruses**, nor is *Walsh* directed to trying to deal with a virus that is found. Rather, *Walsh* is focused on identifying if a file during a file open event contains content, such as a macro or other customizations in a Microsoft Word document, that make that file ***more susceptible to being capable of being infected with a virus***, and allowing the

user to stop the normal opening of the file to confirm that the user wants to accept that risk. (*See* generally the Background of *Walsh*, Col. 1, line13 – Col. 2, line 59.)

Note that *Walsh* is not directed at the problem of detecting viruses and dealing with any viruses that are found, but rather *Walsh* is more narrowly focused on protecting a file or document from virus infection by including protecting within the executable program itself (*see* Col. 2, lines 35-59), such as by having Microsoft Word check to see if a Word document contains macros or customizations, and if so, allowing the user to choose to open the file normally, not open the file, or to open the file in safe mode so that the macros or customizations are not executed. (See Col. 9, line 53 – Col. 10, line16.)

Specifically, *Walsh* explains that Figure 2 shows "a method for protecting a file from infection by a virus" (Col. 6, line 47), that includes: (1) detecting a file open event in step 202; (2) determining whether the selected file **is a *candidate* for virus infection** in step 204; (3) if so, then providing notice to a user to advise that the file is ***susceptible*** to virus infection in step 208; (4) determining whether the user has chosen, in response to the notice, to open the file or not in step 210; and (5) if the user has not chosen to open the file, whether the user has chosen to either cancel opening of the file or open the file in safe mode, in step 212. (See Figure 2; Col. 10, lines 17-56.) *Walsh's* Figure 4C provides an example of the notice given to the user that a document the use is opening "contains macros or customizations…Some macros ***may*** contain viruses that could harm your computer." (See Figure 4C; Col. 12, lines 26-52; emphasis added.)

Significantly, *Walsh* itself clarifies that the techniques therein are ***not*** directed at detecting viruses and acting upon any viruses that are found. *Walsh* explains that "this internal virus check routine **does not scan a memory storage device of a computer to detect and remove viruses**." (Col. 9, lines 59-60; emphasis added.) Instead, Walsh's "routine can support ***presentation of a notice or warning*** message in response to detecting the opening of a document that ***may*** contain a virus [based on the file containing content that is known to be susceptible to being compromised by a virus, such as a Microsoft Word macro]. In response to this notice, the user can select an option for further processing of the document to be opened." (Col. 9, lines 61-65; emphasis added.)

In summary, *Walsh's* approach is not about detecting viruses and acting upon such detections, but rather is about informing a user that a file has an increased risk of being infected based on the type of content of the file (e.g., macros), as opposed to the file's content itself.

(3) THE FINAL OFFICE ACTION'S CITATIONS FROM *WALSH* IN REJECTING CLAIM 1

The Final Office Action states that *Walsh* discloses "a virus protecting process (virus protection system implemented as utility programs, see abstract line 2 and col. 1 lines 40-45) configured to detect that one or more unauthorized instructions (virus, abstract line 8) have been stored on the multi-function peripheral device (see abstract lines 7-8); and in response to detecting that the one or more unauthorized instructions have been stored on the multi-function peripheral device, perform one or more actions (notice offers options, col. 3 lines 59-62) to address the one or more unauthorized instructions that have been stored on the multi-function peripheral device." However, while *Walsh* describes a "virus protection system" (Abstract, line 2), ***Walsh's* approach does not detect viruses**. Rather, *Walsh's* approach "can detect either an external or internal **open file event**" (Abstract, line 3), including "an inquiry…to determine whether the file is ***likely*** to contain a virus" (Abstract, lines 8-9) and if so, "a notice is generated to indicate that the **file *may* contain a v**irus, thereby advising of the possible danger of spreading the virus to other files if the file opening is completed." (Abstract, lines 9-12; emphasis added.)

Thus, *Walsh's* abstract makes clear, contrary to the rejection of Claim 1 in the Final Office Action, that **the *detection* performed by *Walsh* is of a *file open event*, *not* the *detection* a *virus***, and that the notice to the user is generated ***not* upon *detection* of a *virus***, but rather upon determining if the **file** is merely **likely to contain a virus** based on one or more specific types of content in the file, such as a Word document that includes macros, which are known to be capable of being infected with a virus. (See *Walsh*, Background, Col. 1, line 64 – Col. 2, line 34.)

With regards to the Final Office Action's citation to Col. 1, lines 40-45, that portion of *Walsh* is describing that the computer industry has developed utility programs that are separate from executable programs, whereas *Walsh's* approach is "to incorporate virus protecting within the executable program itself" in order to "address external and internal open file events." (Col. 2, lines 53-59.) Thus, *Walsh* is not detecting viruses as in those industry developed, separate utility programs.

With regards to the Final Office Action's citation to Col. 3, lines 59-62, that portion of *Walsh* is describing the notice presented to the user regarding the file open document operation after the file is determined to contain "macros and/or customization routines…[that] can contain certain viruses." (Col. 3, lines 43-48.) Specifically, the notice for the open document operation is described as including the following options: (1) open the document in the 'safe mode;'

(2) proceed with normal opening of document; and (3) cancel the document opening." (Col. 3, lines 59-62). But it is important to recognize that this notice is ***not*** presented to the user in response to detecting a virus, but rather is present in response to a file open event for a file that is determined to have macros and/or customization routines, which are known to capable of containing viruses.

But *Walsh's* approach makes no determination whatsoever of whether that file actually includes a virus, and in fact, if the file does contain a macro-based virus and the user elects to open the file anyway in normal mode (not safe mode), the virus has not been detected, little less neutralized, and therefore, the virus would be capable of acting according to the virus' programming.

In summary, the Applicant respectfully submits that the Final Office Action's reliance upon *Walsh* as disclosing the cited portions of Claim 1 is misplaced because (1) *Walsh* is consistent in describing the techniques therein as a way to protect documents from viruses by identifying whether those documents, when the documents are being opened, contain content that is know to be susceptible of being infected with a virus, such as Word macros including macro-based viruses; (2) *Walsh* expressly teaches away from the approach of Claim 1 by stating that "this internal virus check routine **does not scan a memory storage device of a computer to detect and remove viruses**" (Col. 9, lines 59-60; emphasis added); and (3) thus *Walsh's* approach never determines whether viruses are in the documents, little less taking an action to deal with any viruses that might be present.

Therefore, the Applicant respectfully submits that *Walsh* does not disclose, teach, suggest, or in any way render obvious "a virus protection process…configured to…**detect** that one or more **unauthorized instructions** are stored **on the non-volatile memory** of the multi-function peripheral device" and "**in response to detecting** that the one or more **unauthorized instructions** have been **stored** on the non-volatile memory of the multi-function peripheral device… **perform one or more actions to address the one or more unauthorized instructions** that have been stored on the non-volatile memory of the multi-function peripheral device," as featured in Claim 1.

(4) THE FINAL OFFICE ACTION'S CITATIONS FROM *WALSH* IN REJECTING CLAIMS 6 AND 10

As amended above, Claim 1 now includes features that are the same as or similar to those of Claims 6 and 10, which have been subsequently cancelled in the above claims amendment. As a result, the Applicant is addressing herein the Final Office Action's rejection of Claims 6 and 10, based on the rejections referenced by the Final Office Action in the previous Non-Final Office Action, because those rejections are now relevant to the features of Claim 1 herein.

With respect to the features of Claim 6, the previous Non-Final Office Action states that *Walsh* "discloses a virus protection process (virus protection system implemented as utility program, see abstract line 2 and col. 1 lines 40-45) is configured to examine data stored (col. 8 lines 1-6) on a non-volatile memory (non-volatile storage, col. 8 lines 24-26) of the multi-function peripheral." However, as noted above, *Walsh* expressly teaches away from this feature when *Walsh* states that "this internal virus check routine **does not scan a memory storage device of a computer to detect and remove viruses**" (Col. 9, lines 59-60; emphasis added). And furthermore, as discussed below, there is nothing in the cited portions of *Walsh*, or elsewhere, that disclose these features of Claim 1.

The first set of citations to *Walsh* are already addressed above and apply herein, and therefore, that previous discussion is not repeated here. Regarding the additional citations to Column 6 of *Walsh*, the Applicant respectfully submits that there is nothing disclosed about a virus protection process configured to "examine data stored on non-volatile memory of the multi-function peripheral device," as currently featured in Claim 1 (and previously featured in Claim 6). Specifically, Col. 8, lines 1-6 state: "...frame computers, and the like. The invention may also be practiced in distributed computing environment where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices." While this portion of *Walsh* may be interpreted as disclosing memory storage, there is nothing therein about non-volatile memory, little less the examination of data stored on such non-volatile memory, as featured in Claim 1.

Also, Col. 8, lines 24-26 state: "...face 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage for the personal computer 20." While this portion of *Walsh* does mention non-volatile storage, it says nothing about the examination of data in such non-volatile storage.

With respect to the features of Claim 10, the previous Non-Final Office Action states that *Boldon* describes "a method whereby embedded peripheral devices may be able to detect and otherwise render harmless any such virus that is received by the device (page 2 [0017]), as required by claim 10. Moreover, *Boldon* et al. discloses the step of deleting the information if the information contains a virus and/or contacting the system administrator if a virus is found in the information (page 1 [0007])." The Applicant notes that this is a correct citation of *Boldon*, and further that *Boldon* describes how viruses are rendered harmless, namely by "deleting the information if the information contains a virus…if a virus is found in the information" (paragraph [0007]).

However, the intent of the features of Claim 10 was not to feature the deleting of a virus, because otherwise the Applicant would have phrased the claim with that term. Rather, the intent of Claim 10 was to feature that virus protection process is configured to "render the one or more unauthorized instructions ***inaccessible*** and ***unexecutable*** on the multi-function peripheral device" but without deleting the unauthorized instructions. (Emphasis added.)

Given the previous Non-Final Office Action's interpretation of *Boldon's* disclosure of rendering a virus harmless by deleting the virus, the Application has clarified these features of Claim 10 that are now included in Claim 1 by also featuring that the rendering of the unauthorized instructions inaccessible and unexecutable is done by "moving the one or more unauthorized instructions into a protected area of the non-volatile memory." As discussed above, these additional features of Claim 1 are fully supported by the Application as filed, and no new matter is included.

As a result, the Applicant respectfully submits that Claim 1, as amended, is not disclosed by *Boldon* because deleting a virus as described by *Boldon* is not the same as "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device **by *moving* the one or more unauthorized instructions into a *protected area* of the *non-volatile memory***," as now featured in Claim 1. In fact, *Boldon's* teaching of the deletion of a virus expressly teaches away from this feature of Claim 1 in which the unauthorized instructions are moved into a protected area of non-volatile memory, not deleted as in *Boldon's* approach.

(5) DISCUSSION OF CLAIM 1 AND *PHAN* AND *CHEN*

While *Phan* and *Chen* are not relied upon as disclosing the features of Claim 1 discussed above, the Applicant notes that neither *Phan* or *Chen*, either alone or in combination with each other and/or with *Walsh* and/or *Boldon*, do not disclose, teach, suggest, or in any way render obvious "a virus protection process…configured to…**detect** that one or more **unauthorized instructions** are stored **on the non-volatile memory** of the multi-function peripheral device" and "**in response to detecting** that the one or more **unauthorized instructions** have been **stored** on the non-volatile memory of the multi-function peripheral device… **perform one or more actions to address the one or more unauthorized instructions** that have been stored on the non-volatile memory of the multi-function peripheral device," "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device **by *moving* the one or more unauthorized instructions into a *protected area* of the *non-volatile memory***," as now featured in Claim 1.

In addition, the Applicant notes that the Final Office Action states that *Phan* discloses "a graphical user interface (User Interface, col. 3 lines 20-28, Fig. 2)," but that upon a careful reading of that portion of *Phan* and examination of Figure 2, the only user interface disclosed is not described as a "graphical" user interface and would most reasonably be interpreted as a command line interface, not a GUI. The Applicant also notes that the Final Office Action states that *Phan* discloses "a scan process…executing in the memory (col. 4 lines 14-16)," but this cited portion of Phan actually describes that the "control unit 110*b* includes management software stored in the long term memory 280 for managing print jobs, fax jobs and scan jobs..," which would be understood to be non-volatile storage that would be incapable of having "a scan process…executing" therein, since such executing generally occurs in volatile memory, such as RAM, not in a "disk" as element 280 is illustrated in Figure 2 of *Phan*.

(6) DISCUSSION OF "DICTIONARY" REJECTIONS WITH RESPECT TO CLAIM 1

As stated in MPEP § 2143.03: "To establish prima facie obviousness of a claimed invention, ***all the claim limitations*** must be taught or suggested by the prior art." *In Re Royka*, 180 USPQ 580 (emphasis added). "***All words in a claim must be considered*** in judging the patentability of that claim against the prior art." *In re Wilson*, 165 USPQ 494, 496 (emphasis added).

The Applicant admits to being perplexed about how to respond to the inconsistency between (1) the evidence required to support an obviousness rejection and (2) the evidence that has been offered in the Office Actions relating to the present application (hereafter, the "Office Actions"). Specifically, to support an obviousness rejection, the Applicant would expect an argument that has the following form: (1) element X is shown in reference A, (2) element Y is shown in reference B, and (3) there is some actual suggestion to combine the references A and B to create the mechanism or technique that has both elements X and Y.

However, the Office Actions for the present Application do not support the obviousness rejections in that manner. Rather, to support the obviousness rejections, not only has each claim been divided into its constituent elements, but also each constituent element of the claim has been finely dissected into a set of short phrases and sentence fragments. The Office Actions then point out how each individual fragment corresponds to a similar fragment in any one of a handful of references using inappropriate hindsight-based analysis, without reading and incorporating into the rejection the context in which those terms are used within the claims.

For example, as discussed above, the previous Non-Final Office Action rejection of Claim 6 appears to be based solely on the citations to *Walsh* that disclose "non-volatile storage," but the additional feature of Claim 6 is not just "non-volatile storage" but "examine data stored on a non-volatile memory." Yet the cited portions of *Walsh* are silent as to such an examination. Instead, the Applicant would expect that the cited portion of a reference would show the entire feature of the claim that is being recited by the Office Actions, not just a key word or phrase of that feature. At a minimum, the Application would expect to find a discussion of how the Office Actions are interpreting the disclosure of such a keyword or phrase as disclosing the entire feature being recited.

Such a piecewise dissection of a claim word by word, or term by term, using different and unrelated portions of a reference or even multiple references, could be logically extended to doing so for all the words of a claim. Thus, a claim that includes preexisting words could therefore be rejected based solely on a dictionary that discloses all of those words without referencing any specific prior art teachings of the steps, techniques, and features included in a claim. Yet the Applicant hopes that the Office would agree that issuing 102 rejections of claims based on the fact that all the words appear in a dictionary would not be the proper basis to support a 102 rejection. In short, the Applicant respectfully submits that Office Actions should

be based on finding the "features" of a claim within one or more prior art references, and not on merely finding within the prior art references the individual "words" or "terms" used to describe those features in the claim.

(7) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *WALSH, BOLDON, PHAN*, AND *CHEN*

Because *Walsh, Boldon, Phan*, and *Chen*, either alone or in combination, fails to disclose, teach, suggest, or in any way render obvious "a virus protection process…configured to…**detect** that one or more **unauthorized instructions** are stored **on the non-volatile memory** of the multi-function peripheral device" and "**in response to detecting** that the one or more **unauthorized instructions** have been **stored** on the non-volatile memory of the multi-function peripheral device… **perform one or more actions to address the one or more unauthorized instructions** that have been stored on the non-volatile memory of the multi-function peripheral device," "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device **by *moving* the one or more unauthorized instructions into a *protected area* of the *non-volatile memory***," as now featured in Claim 1, the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIM 17

(1) INTRODUCTION TO CLAIM 17

Claim 17 features:

"A multi-function peripheral device comprising:

a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;

a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;

one or more processors;

a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of a first electronic document that is based on the printed document;

a print process executing in the memory and being configured to process print data and cause a printed version of a second electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured to, ***upon receipt* of data by the multi-function peripheral device from a network device over the network**, perform the steps of:

examine the data to determine whether the data contains one or more unauthorized instructions;

in response to determining that the data contains one or more unauthorized instructions, perform one or more actions on the data to protect the multi-function peripheral device;

wherein the one or more actions includes **rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving* the one or more unauthorized instructions into a *protected area* of non-volatile memory**." (Emphasis added.)

Thus, Claim 17 includes many features that are the same as or similar to Claim 1, although there are many features of Claim 17 that differ from Claim 1. For example, Claim 1 features examining data stored on non-volatile memory of the multi-function peripheral and based on that examination detecting that one or more unauthorized instructions are stored thereon. In contrast, Claim 17 features the virus protection process being configured to perform several steps ***upon receipt*** of data by the multi-function peripheral device, instead examining data stored in non-volatile memory as in Claim 1. As an example of similarities between Claim 1 and Claim 17, both feature "the one or more actions includes **rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving* the one or more unauthorized instructions into a *protected area* of non-volatile memory**."

Newly added Claim 17 is fully supported by the Application as filed, and no new matter is included. For example, the features of "a network interface…," a graphical user interface…," one or more processors," "a memory," "a scan process…, and "a print process…" are either the

same as or similar to those of Claim 1. As noted above, in Claim 17, the "virus protection process" is configured to perform steps "upon receipt of data…," which is supported by at least Section VIII of the Application on page 19 et seq., which describes an embodiment referred to as "intruder detection" in which data received by MFPs is checked for viruses, such as by scanning a print job or configuration data received by the MFP, and if a virus is detected, repairs, quarantines or deletes the data. (Application, paragraph [0046] et seq.) Also, as discussed above, Claim 17 includes the feature of "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving*** **the one or more unauthorized instructions into a *protected area* of non-volatile memory**," which is supported by the same portions of the Application discussed above with reference to the same feature of Claim 1.

(2) DISCUSSION OF CLAIM 17 AND *WALSH, BOLDON, PHAN*, AND *CHEN*

As noted above, Claim 17 is similar to Claim 1 in that both feature "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving*** **the one or more unauthorized instructions into a *protected area* of non-volatile memory**." The Applicant has previously addressed these features with respect to the cited art, and therefore the Applicant respectfully submits that Claim 17 is allowable over the prior art for at least the same reasons as those given above with respect to this feature for Claim 1.

D. CLAIM 20

(1) INTRODUCTION TO CLAIM 20

Claim 20 features:

"A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;
one or more processors;
a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of a first electronic document that is based on the printed document;

a print process executing in the memory and being configured to process print data and cause a printed version of a second electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured, ***prior to sending*** **data from the multi-function peripheral device to a network device over the network**, to perform the steps of:

examine the data to determine whether the data contains one or more unauthorized instructions; and

in response to determining that the data contains one or more unauthorized instructions, perform one or more actions." (Emphasis added.)

Thus, Claim 20 includes many features that are the same as or similar to Claim 1, although there are many features of Claim 20 that differ from Claim 1. For example, Claim 1 features examining data stored on non-volatile memory of the multi-function peripheral and based on that examination detecting that one or more unauthorized instructions are stored thereon. In contrast, Claim 20 features the virus protection process being configured to perform several steps ***prior to sending*** data from the multi-function peripheral device to a network device over a network, instead of examining data stored in non-volatile memory as in Claim 1. As an example of similarities between Claim 1 and Claim 17, both feature "the one or more actions includes **rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving*** **the one or more unauthorized instructions into a *protected area* of non-volatile memory**."

Newly added Claim 20 is fully supported by the Application as filed, and no new matter is included. For example, the features of "a network interface...," a graphical user interface...," one or more processors," "a memory," "a scan process..., and "a print process..." are either the same as or similar to those of Claim 1. As noted above, in Claim 20, the "virus protection

process" is configured to perform steps "prior to sending data from the multi-function peripheral device to a network device over a network," which is supported by at least Section VIII of the Application on page 19 et seq., which describes an embodiment referred to as "check on send" in which virus checking is performed on data that is to be sent, such as by email, from the MFP to other locations or devices over a network, and if the email is determined to be infected with a virus, then the email is not sent. (Application, paragraph [0047] et seq.) Also, as discussed above, Claim 20 includes the feature of "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving*** **the one or more unauthorized instructions into a *protected area* of non-volatile memory**," which is supported by the same portions of the Application discussed above with reference to the same feature of Claim 1.

(2) DISCUSSION OF CLAIM 20 AND *WALSH, BOLDON, PHAN*, AND *CHEN*

The Applicant respectfully submits that none of *Walsh*, *Boldon*, *Phan* or *Chen*, either alone or in combination, disclose, teach, suggest, or in any way render obvious "a virus protection process executing in the memory and being configured, ***prior to sending*** **data from the multi-function peripheral device to a network device over a network**, to perform the steps of… examine the data to determine whether the data contains one or more unauthorized instructions; and in response to determining that the data contains one or more unauthorized instructions, perform one or more actions," as featured in Claim 20.

In particular, while *Phan* discloses an MFP, *Phan* is silent as to anything akin to virus checking. Regarding *Walsh*, the Applicant has explained at length above why *Walsh* fails to disclose virus checking as well.

As for *Boldon*, the approach therein for virus filtering in peripherals is limited to scanning, at a printer, information that is sent ***to*** the printer before the printer print the information, which is the opposite of Claim 20 in which data, ***prior to being sent*** **from** the *multi-function peripheral device* **to** *a network device*, is examined for unauthorized instructions.

As for *Chen*, the approach therein for detecting and removing viruses located in attachments to email messages is used when such emails are received at a database or mail server, not "***prior to being sent*** **from** the *multi-function peripheral device* **to** *a network device*, as in Claim 20.

Also, as noted above, Claim 17 is similar to Claim 1 in that both feature "**rendering the one or more unauthorized instructions inaccessible and unexecutable** on the multi-function peripheral device ***by moving*** **the one or more unauthorized instructions into a *protected area* of non-volatile memory**." The Applicant has previously addressed these features with respect to the cited art, and therefore the Applicant respectfully submits that Claim 17 is allowable over the prior art for at least the same reasons as those given above with respect to this feature for Claim 1.

E. CLAIMS 2-3, 8-9, 11, 15-16, 18-19, AND 21-28

Claims 2-3, 8-9, 11, and 15-16 are dependent upon Claim 1, Claims 18-19 are dependent upon Claim 17, and Claims 21-28 are dependent upon Claim 20, and thus each of Claims 2-3, 8-9, 11, 15-16, 18-19, and 21-28 include each and every feature of the corresponding independent claims. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2-3, 8-9, 11, 15-16, 18-19, and 21-28 are allowable for the reasons given above with respect to Claims 1, 17, and 20.

(2) SUPPORT FOR NEWLY ADDED DEPENDENT CLAIMS FOR INDEPENDENT CLAIMS 17 AND 20

Newly added dependent Claim 18 depends on Claim 17, and newly added dependent Claims 21-25 and 27-28 depend on Claim 20. These added claims are fully supported by the Application as filed, and no new matter is included.

For example, newly added Claims 18 and 22 feature different types of notification, which are similar to previously included Claim 11 (which, as amended above, combines features originally included in several different claims, namely Claims 12-14, which have subsequently been cancelled).

As another example, Claims 24 and 25 include features about undoing changes and deleting data if the data cannot be restored to a prior state, respectively, which are the same as or similar to previously included Claims 8 and 9, respectively.

Finally, Claims 18, 21-25, and 27-28 are based on claims originally filed in related application S/N 10/776,486, which has the same specification and drawings as the present

Application, and which is incorporated by reference in paragraph [0001] by the present Application.

(2) CLAIMS 16, 19, AND 26

Newly added dependent Claim 16 depends on Claim 1, newly added dependent Claim 19 depends on Claim 17, and newly added dependent Claim 26 depends on Claim 20. These added dependent claims are fully supported by the Application as filed, and no new matter is included.

For example, the Application describes an embodiment in paragraph [0031] in which some deletion operations may only remove the name of an infected application program from a file attribute table (FAT), and therefore to ensure that the infected application program is permanently deleted from the MFP, the "virus protection tool 108 may 'scrub' a portion of non-volatile storage 106 where the particular application program was stored by overwriting the portion of non-volatile storage 106 with a specified value or pattern, such as 0H.

In addition, the Applicant respectfully submits that none of *Walsh*, *Boldon*, *Phan* or *Chen*, either alone or in combination, disclose, teach, suggest, or in any way render obvious "the one or more unauthorized instructions are contained in a file stored on a portion of the non-volatile memory," "the one or more actions includes deleting the file," "the virus protection process is further configured to, after deleting the file, overwrite the portion of the non-volatile memory with a specified pattern," as featured in Claims 16, 19, and 26.

CONCLUSION

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments and further examination on the merits are respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/CraigGHolmes#44770/

Craig G. Holmes
Reg. No. 44,770
Date: September 6, 2007

2055 Gateway Place, Suite 550
San Jose, CA 95110
(408) 414-1204
Facsimile: (408) 414-1076